AIR WAR COLLEGE

AIR UNIVERSITY

CYBER THREAT AWARENESS FOR THE WARFIGHTER

by

Jason R. Settle, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Mr. Michael P. Ivanovsky

16 February 2016

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lt Col Jason R. Settle entered the United States Air Force in 1997 after receiving his commission from the 305th ROTC Detachment at Louisiana Tech University. He is a command pilot with more than 2,000 total flying hours in the F-15C and T-38C including 91 combat hours. He completed Specialized Undergraduate Pilot Training (SUPT) at Laughlin AFB, Texas and fighter training in the F-15C at Tyndall AFB, Florida. His operational F-15C assignments were at Langley AFB, Virginia and Kadena Air Base, Japan. His T-38C assignments include an Introduction to Fighter Fundamentals (IFF) instructor tour at Moody AFB, Georgia and as the Commander, 50th Flying Training Squadron at Columbus AFB, Mississippi.

Abstract

The United States Air Force has placed increasing emphasis on cyber in recent years, but most of this has been on defending network operations and information technology infrastructure. However, the aircraft used to deliver weapons in combat operations would also be a logical target of cyber operations by our adversaries. If aircraft can be targeted or are vulnerable to cyber threats, then operators should be aware of these threats. This paper explores to what extent cyber threat education can help bridge the gap between aircraft operators and cyber experts in order to mitigate risks to Air Force missions. The resulting research demonstrates there are benefits to educating warfighters, specifically fighter aircrew, on cyber to mitigate the potential risks cyber threats pose. Several recommendations on how to accomplish cyber threat education for the warfighter are presented.

Introduction

The United States Air Force has placed increasing emphasis on cyber during the past decade. In 2005, the Air Force codified the importance of cyberspace by including it in the service's mission statement - Fly, Fight and Win...in Air, Space and *Cyberspace*. Additionally, the Department of Defense (DoD) stood up USCYBERCOM in 2010, a new sub-unified command focused on cyber. These are significant steps towards grappling with cyber challenges in the military, but most of the initial focus has been on defending network operations and information technology (IT) infrastructure with limited progress on how cyber threats can affect weapons systems such as aircraft. Given the DoD's reliance on computer networks, this network-centric approach to cyber threats is understandable. However, aircraft that deliver weapons in combat operations are also logical targets of cyber operations by our adversaries. Examining cyber threats to aircraft is an example of what Maj Gen Vautrinot, former 24 AF/CC, was referring to when she wrote that the "emphasis is on supporting operational missions dependent on cyberspace" and "the focus is on the mission, not the network."[1] Joint Publication 1-02 defines cyberspace as "a global domain…consisting of the interdependent network of IT infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2] Modern fighter aircraft have many "embedded processors and controllers" that are susceptible to cyber threats.[3] If aircraft are vulnerable to cyber threats, then operators should be aware of these potential threats. This paper seeks to explore to what extent cyber threat education for the warfighter can help bridge the gap between aircraft operators and cyber experts in order to mitigate risks to Air Force missions. The resulting research will demonstrate

that there are benefits to educating warfighters, specifically fighter aircrew, on the potential risks cyber threats pose so they can be mitigated. Several recommendations on how to accomplish cyber threat education for the warfighter are presented.

Need for Warfighter Cyber Threat Awareness

The Air Force's Chief Information Officer, Lt Gen William Bender, provides the following vector summarizing the need for cyber threat education in his 2015 Information Dominance Flight Plan:

> Further develop and implement education and training programs to raise awareness of cybersecurity threats to core missions – this includes educating and informing all Airmen and industry partners on how malicious software (malware) can infest mission/weapon systems platforms. Prevention and education is crucial to achieve lasting success and change in Air Force culture and how we address cybersecurity. This line of effort will focus on ensuring all Airmen not only get the right training, but also the supportive intelligence information to make the right decisions.[4]

The underlying assumption here is that the impacts of cyber threats to our computer networks are being addressed, but better awareness is needed regarding the mission impacts of cyber threats to our weapons systems. Kamal Jabbour and Sarah Muccio assert "the development of weapons in the current arsenal did not take into account a contested cyber environment…and missed opportunities to identify and mitigate cyber vulnerabilities in critical missions."[5] Cyber threat awareness is especially important for the aircraft operators who employ capabilities that are vulnerable to cyber threats. Although there is not yet a fully enumerated list of cyber vulnerabilities for every Air Force aircraft, raising the awareness of warfighters to possible cyber threats and how an adversary might exploit typical vulnerabilities is a critical first step in mission assurance. For example, aircraft maintenance crews "routinely connect these weapons systems to

maintenance devices that are conduits to the wider cyberspace world."[6] This typical vulnerability may be common, but it is not commonly addressed. Cyber threats cannot be treated as "someone else's job" because no one else better understands the potential impacts of cyber threats for a given weapons system than the operators who are tasked with flying the airplane to carry out the mission.

Writing on the future of cyber warfare, Col William Poirier and Maj James Lotspeich posit that eventually advances in the Air Force's cyber organization and operations "will free DODIN [DoD Information Network] operators to concentrate on defensive hardening and attack recovery while expanding their scope to nontraditional networks."[7] What compromises nontraditional networks? Col William Bryant offers a salient explanation when he writes "nontraditional and platform IT is increasingly referred to as Operational Technology or OT as opposed to IT…An F-16 fighter or M-1 Abrams tank is in this category."[8] Like others, Bryant also sees the need "for the Department of Defense (DoD) to extend our own active cyberspace defenses beyond traditional IT networks and into mission and weapons systems."[9] Expanding the scope of cyber operations beyond traditional networks may also help to break down "domain-centric stovepipes"[10] and facilitate better cross talk between air domain operators (such as fighter aircrew) and cyber domain operators. Yet, presently, the understanding and communication of cyber threats to aircraft operators in a meaningful way is lacking. Consequently, there is a lack of attention to cyber threats by the warfighter, resulting in a de facto and dangerous assumption that mission execution will not be hindered by cyber threats. Understanding cyber threats to aircraft systems and their potential impacts to the mission is essential if we are to mitigate the threat. This can be accomplished by

providing a tailored message to operators along with the latitude to make their own risk assessment.

In order to identify the level of cyber threat awareness in Air Force operational flying squadrons, interviews were conducted with instructor pilots and squadron commanders from F-15C, F-16, F-22, and A-10 units (see Appendix interviewee demographics and interview questions). The results of these interviews illustrated a predictable lack of awareness for cyber threats to their respective weapons systems. In fact, when asked about the general level of cyber awareness in fighter squadrons, most answers remained focused on the aspect of cyber threats to the network. A follow-up question was posed about the need for awareness on cyber threats to weapons systems, which elicited responses that can be characterized by a belief that there is not a significant cyber threat to Air Force aircraft or that if there were a threat, the cyber experts would handle it. This is unfortunate because the aircrew operating and employing aircraft on a daily basis should be aware of potential threats that can impact their ability to conduct the mission. Aircrews currently get a variety of threat information during initial weapons systems training and regular updates from embedded squadron intelligence personnel. However, the threat intelligence provided is primarily limited to kinetic threats such as adversary aircraft, surface-to-air missiles/guns, and air-to-air missiles/guns. The rise of cyber threats and the affect they can have on aircraft systems has not yet been fully incorporated into initial training for aircrew or intelligence personnel.

One notable effort to remedy this knowledge deficiency is where Red Flag has begun to incorporate cyber threats into exercises during the past couple of years in an

effort to expose aircrew to the adverse effects a cyber attack might have.[11] Those interviewed remarked the Red Flag cyber aspect was beneficial, but was also somewhat of a novelty and they did not typically consider cyber aspects after returning from the exercise. Therefore, while Red Flag's initial efforts make an important contribution in cyber threat education, this does not address the absence of cyber threat awareness at home station where aircrew spend the majority of their time training.

This naturally leads to a lack of cyber threat awareness by aircrew, which means aircrew unknowingly accept risk in the missions they conduct. It is understood that our Airmen will be exposed to various risks; however, they should be aware of those risks even if they cannot be mitigated. Regarding kinetic threats, the Air Force addresses this by teaching aircrews how to recognize these threats and what the enemy's capabilities are. This essential knowledge of kinetic threats empowers aircrew to avoid or defeat them in combat. Despite the significant differences between kinetic and cyber threats, this line of reasoning holds true for cyber threats in several fundamental ways.

Benefits of Cyber Threat Awareness

First, an understanding of cyber threats to one's aircraft would help aircrew to avoid threats to the extent they have control over. This can be compared to how aircrew are taught about the capabilities and location of an enemy surface-to-air missile (SAM) system so they can avoid the threat by not flying into its effective range. Likewise, since aircrew directly interact with the aircraft and the computer systems that support and transfer data to the aircraft, understanding relevant cyber threats can help them avoid actions that might open an avenue for a cyber threat to exploit. Operating procedures are typically constructed to facilitate cybersecurity, but it is not enough to rely solely on

procedural adherence to address the ever-evolving world of cyber. One advantage of having aircrew understand cyber threats is that when they understand the "why" behind a procedure, they are more likely to follow it. Additionally, and more importantly, understanding the "why" behind a procedure allows aircrews to make better choices when the situation does not fit the procedure exactly. The fact that aircrew deal directly with their aircraft makes them well suited to detect avenues that are vulnerable to cyber threats, but only if they have an understanding of the threat to begin with. Without an understanding, aircrew are prone to assume that there is no real cyber threat to their aircraft or that someone else is taking care of cybersecurity. Both of these assumptions are incorrect and reveals why cyber threat education can help mitigate cyber risks to the mission.

Second, understanding the cyber threat may also allow aircrew to defeat a cyber threat that has been deployed against their aircraft. Returning to the analogy of kinetic threats, aircrew cannot always avoid enemy SAM systems and are therefore taught maneuvers designed to defeat them. Similarly, all cyber threats cannot be simply avoided and may require aircrew actions to assist in defeating them. As opposed to kinetic threats, cyber threats can be subtle and difficult to defeat even when identified. Still, there may be indicators when a cyber threat has actually compromised an aircraft system and aircrew should be one of the first to recognize these indicators. Without an understanding of those indicators, aircrew might overlook seemingly innocuous cockpit indications, thus allowing a cyber attack to go unnoticed until it is too late. There might be immediate actions the aircrew can take when they suspect a cyber attack, but only if they are educated on what to look for. Even if the cyber attack cannot be immediately

defeated, aircrew who recognize the attack can bring that information back after the mission so cyber experts can begin mitigation measures. Overall, aircrew properly educated on cyber threats can help mitigate cyber risks to the mission in a number of ways.

Potential Cyber Threat Education Initiatives

With an understanding of the benefits cyber threat education provides, the next step is to determine what can be done to improve cyber threat awareness. The ideal solution is institutionalization of cyber into all mission areas involving all Airmen so that cyber is a norm taught in each stage of training. Although centered on network security, the idea of instilling a culture of cyber awareness was clearly expressed when the Chairman of the Joint Chiefs of Staff and Secretary of Defense released the DoD Cybersecurity Culture and Compliance Initiative (DC3I) in September 2015. The DC3I states that knowledge "enables all of the other principles" in cybersecurity and as such, "the greater our collective competency in cyberspace, the better prepared we are to mitigate risk, make smart decisions, and achieve mission objectives during an unauthorized DODIN [DoD Information Network] intrusion."[12] To gain this collective competency, the DC3I mandates extensive training for all DODIN users and the incorporation of "DC3I principles into all levels of training, including, but not limited to accession pipelines, professional development, and leadership development."[13] In other words, the military's most senior leaders are directing a comprehensive institutionalization of network cybersecurity awareness for all DoD members. This guidance is congruent with efforts to educate warfighters on aircraft cyber threats and encompasses many of the cyber threat awareness principles already covered in this paper.

The overarching need for institutionalized cyber threat training in formal aircrew courses could be handled in the same manner kinetic threats are institutionalized. Likewise, institutionalized cyber threat training is needed for intelligence personnel who already brief aircrew on kinetic threats. Institutionalizing cyber threat training is consistent the USAF Strategic Master Plan, which identifies the need to "institutionalize multi-domain approaches into the education, training, and employment of Airmen from the operator to the component commander."[14] These two lines of effort, teaching aircrew and intelligence personnel, would provide a basic level of cyber threat awareness needed in flying squadrons. Furthermore, flying squadrons could designate an operator to be the "cyber officer" as an additional duty. However, since cyber threats evolve rapidly, there is also a need for dedicated cyber expertise within the flying wings. This expertise would likely come from the Cyber Squadron of the future. The Cyber Squadron of the future will provide cyber support tailored to the wing's mission and be postured to work in coordination with aircraft operators (amongst all other missions across the wing) in countering cyber threats with the goal of providing mission assurance.[15] Cyber threat awareness among aircrew, intelligence personnel, and Cyber Squadron personnel will provide embedded cyber awareness throughout a wing's mission making it integral to daily business rather than an afterthought. Still, this solution does not address legacy aircrew and intelligence personnel already trained, and the Cyber Squadron of the future is not scheduled for implementation until 2018.[16]

In the interim, there are options that can be implemented to remedy the lack of cyber threat awareness in flying squadrons. The first option is the dissemination of cyber threat intelligence via the existing intelligence personnel in the flying squadrons. Second,

the development of resident courses on cyber threats for aircrew. Third, a cyber threat roadshow delivered to aircrew at their home station. These options are not all inclusive and each has its own pros and cons. Yet, these options represent avenues that are executable in the short term without disrupting the long-term solution of institutionalized cyber training.

First of all, delivering cyber threat information via intelligence personnel organic to the flying squadron affords several benefits. With intelligence personnel already incorporated into the flying squadrons, there are no additional manpower requirements. This assumes the additional cyber threat training will be kept to a reasonable level and not over-tax personnel. The advantage of this approach is that intelligence personnel already have an existing rapport with aircrew. Aircrew are used to receiving threat information from their intelligence experts and would be more likely to trust them with new training requirements. Aircrew are often skeptical of mass education programs directed down from on high. Furthermore, squadron intelligence personnel understand how to customize a cyber threat education message so that it is relevant to the particular aircraft they support.

The challenges of utilizing the squadron intelligence shop for educating aircrew include increased workload and the lack of cyber threat training for intelligence personnel. The increased workload comes from adding cyber threat training requirements for squadron intelligence personnel without adding manpower. Additional manpower would be ideal, but is not likely. Still, communicating cyber threats should not be too tasking and progresses toward institutionalized cyber threat training for intelligence personnel. The lack of cyber training for intelligence personnel is more

problematic, because we are asking one untrained group to train another untrained group. To overcome this problem, the delivery of cyber threat information/intelligence would be mainly limited to prepared material produced by cyber threat experts. These challenges are somewhat limiting, but the canned delivery option still has the potential to be an effective short-term solution, which can lead to long-term institutionalization of cyber threat training for intelligence personnel and aircrew.

Turning to the second idea of a resident course on cyber threats for aircrew presents some unique benefits. The concept proposed here is similar to existing opportunities for aircrew to attend short (1-2 week) residence courses on topics such as electronic warfare systems (Fighter Electronic Combat Officer Course) or air-to-air missiles (Raytheon Systems Warfighter School). Courses like these afford individual aircrew members the chance to return to their squadron as a subject matter expert (SME). In turn, as the cyber threat SME, they would be expected to brief and educate the rest of the squadron as well as being the "go-to" person whenever there is a question on cyber threats. They could also serve as the additional duty "cyber officer". This does not mean they would know everything about cyber, but they would serve as a squadron conduit for cyber issues. The development of a course on cyber threats to aircraft could focus on educating a select number of aircrew who in turn train their squadron members. If employed on a continual basis where squadrons send aircrew for training at regular intervals, this method could afford the opportunity for a cyber threat course to develop over time so that the flying community is kept up to date on the latest known threats. Educating aircrew directly with a course developed for them provides the element of relevancy and keeps the option affordable for the flying squadrons.

Conversely, utilizing the option of resident cyber courses for aircrew would require preparation and resources. The location, instructors, and course material all require development. There will be a resource bill to pay in both funding and manpower. Choosing a location that already has cyber threat expertise and aircrew training expertise would help minimize these challenges while maximizing aircrew training. For example, Nellis AFB is an ideal location for such a course. Home to the 57th Adversary Tactics Group (57th ATG) that oversees the 57th Information Aggressor Squadron (57th IAS), Nellis already provides realistic cyber threat training to aircrew during Red Flag exercises. Furthermore, the 57th ATG also hosts the 507th Air Defense Aggressor Squadron (507th ADAS) which teaches Air Combat Command's Fighter Electronic Combat Officer Course (FECOC). In their Air and Space Power Journal article, Lt Col Scott Bonzer and Lt Col Daniel Bourque describe how the 57th ATG has expanded their threat training to include cross-domain threats stating that "as the Air Force's mission has expanded to include space and cyber operations, the Aggressor mission has broadened to include total-force information aggressor and space aggressor squadrons that provide an integrated, full-spectrum threat alongside their air and air-defense comrades in the 57th Adversary Tactics Group."[17] Combining the capabilities of the 57th IAS and the 507th ADAS could leverage present cyber expertise and experience. At this time, there is a portion of the FECOC course that discusses cyber threats, but it is only a single day and limited in scope. Growing a dedicated cyber course from these initial efforts is the next logical step in advancing cyber threat education efforts. The 57th IAS squadron commander and former 507th ADAS squadron commander were consulted during the development of this approach.

Third, cyber threat education could be delivered with a "roadshow" where mobile training team cyber threat experts visit the Combat Air Forces (CAF) squadrons. Similar to the resident course, a possible source of proficiency for a cyber threat roadshow lies with the 57th ATG at Nellis. Another roadshow source could be Air University's newly established Cyber College, which already plans to offer tailored cyber education to units that require the training. A roadshow has the advantage of allowing the experts to educate a wide audience and deliver current information. It also provides a chance for squadron members to ask questions directly to cyber experts and facilitates crosstalk, which is frequently the genesis of innovative ideas. However, a roadshow does not afford ongoing updates unless it is conducted on a recurring basis. A repeated circuit of cyber threat training roadshows would be time consuming if it covered all CAF squadrons. So, a cyber threat training roadshow could be good for an initial effort to reach a significant portion of the CAF, but might prove cost prohibitive in the long run.

Recommendations

In light of the overall lack of cyber threat awareness among fighter aircrew and the resulting risks, it is clear cyber threat education for the warfighter is greatly needed. Considering the options presented thus far along with the pros and cons of each, this paper recommends the first step be development of a cyber roadshow to initiate cyber threat education efforts followed by the development of a resident course. The roadshow would provide for quick cyber threat education to a large audience and help raise collective awareness and emphasize the importance of cyber. The resident course on cyber threats could provide advanced and evolving cyber education for CAF aircrew. As outlined earlier, Nellis and the 57th ATG should be seriously considered to host both of

these efforts. Air University's Cyber College is also an option, but the 57th ATG's edge lies in its long history of educating warfighters in exercises, vast experience in studying threats, and present ability to rapidly build on their existent courses and capabilities to deliver both the roadshow and a resident course in a coordinated fashion.

Resourcing the initiative is key. The required manpower resources would be modest, but cyber manning is stretched extremely thin DoD-wide. The 57th IAS is no exception. Additionally, temporary duty (TDY) funding is scarce due to current fiscal constraints. Regardless, we should not expect our Airmen to do more without the requisite resources. We need to improve cyber threat awareness so that warfighters know how their aircraft may be compromised by an adversary's cyber attack. If we are serious about cyber threat mitigation, then resources must be allocated accordingly.

Disseminating cyber threat information to fighter aircrew via intelligence personnel is a viable option, but the immediate action should be developing a roadshow and resident course. This is primarily due to the momentum the 57th ATG already has in cyber threat education for the warfighter. Still, there may be additional benefits to a similar education plan for intelligence personnel, which may serve as an area of further research. Education plans for other weapons systems and aircraft other than fighter aircraft are also relevant areas for further research.

Simultaneously with a cyber roadshow and resident course, the long-term solution of institutionalizing cyber threat training for fighter aircrew and intelligence personnel must begin. Cyber threats will only become more prevalent and all Airmen should contribute to an Air Force instilled with cyber mindedness. These steps will ensure future generations understand how cyber touches almost all aspects of the Air Force

mission and why it is so critical to mitigate all cyber threats. A detailed plan for how cyber threat training can be institutionalized is a candidate topic for further research.

Conclusion

In conclusion, this paper has explored how cyber threat education for the warfighter can help bridge the gap between aircraft operators and cyber experts in order to mitigate risks to Air Force missions. Cyber threat awareness among fighter aircrew is insufficient and adds a dimension of risk to mission accomplishment. Several possible methods of conducting cyber threat education for fighter aircrew include the development of a cyber roadshow in the near term coupled with a resident cyber course in the long term. The ultimate cyber threat education goal should be institutionalized cyber in the training programs for fighter aircrew and the intelligence personnel who support them. These actions are an essential part of the broader appreciation for cyber, which spans across all of the Air Force's core missions. It is a daunting task to handle the multitude of facets cyber has brought to every aspect of our operations, especially when cyber threats are constantly changing. Yet, progress is achievable and essential if we are to keep pace with our adversaries in cyberspace. Future developments in cyber technologies and force structure will affect how things develop, but proactive measures are needed now since cyber threats to our weapons systems will be prevalent for the foreseeable future.

Appendix

Interview Questionnaire and Demographics

Interview Questionnaire

1. What is your estimation of cyber awareness in CAF (considering both home station ops and exercises like Red Flag)?

2. Should there be a better awareness of cyber threats to our weapons systems? If yes, what suggestions do you have on what should be done to improve awareness?

3. Should there be a better awareness of what cyber can do during combat operations? If yes, what suggestions do you have on what should be done to improve awareness?

Interview Demographics

5 fighter pilots consisting of a F-16 Squadron Commander, F-15C Squadron Commander, F-22 Instructor Pilot, A-10 Instructor Pilot, and F-16 Instructor/Aggressor Pilot.

Notes

[1] Suzanne M. Vautrinot, "Sharing the Cyber Journey," *Strategic Studies Quarterly* (Fall 2012): 79-80, http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf.

[2] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010, 58.

[3] Col William D. Bryant, "Defending the Walls: Active Cyber Defense of Mission and Weapons Systems," (working paper, 14 Sept 2015), 2.

[4] Lt Gen William J. Bender, *Air Force Info Dominance Flight Plan: The Way Forward for Cyberspace/IT in the United States Air Force*, 1 May 2015, 30, http://www.safcioa6.af.mil/shared/media/document/AFD-150610-015.PDF.

[5] Kamal Jabbour and Sarah Muccio, "On Mission Assurance," in *Conflict and Cooperation in Cyberspace*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton, FL: Taylor & Francis, 2014), 109.

[6] Bryant, "Defending the Walls," 3.

[7] Col William J. Poirier and Maj James Lotspeich, "Air Force Cyber Warfare - Now and the Future," *Air and Space Power Journal* 27, no. 5 (September-October 2013): 87, http://www.airpower.maxwell.af.mil/digital/pdf/issues/2013/ASPJ-Sep-Oct-2013.pdf.

[8] Bryant, "Defending the Walls," 3.

[9] Ibid, 2.

[10] Shawn Brimley, "Promoting Security in Common Domains," *Washington Quarterly* 33, no. 3 (July 2010): 121, doi:10.1080/0163660X.2010.492725.

[11] Staff Sgt. Michael Charles, "Hacking away at tomorrow's threats: Red Flag incorporates cyber domain," 99th Air Base Wing Public Affairs news release, 6 March 2013, http://www.nellis.af.mil/news/story.asp?id=123338589.

[12] Gen Martin E. Dempsey and Hon. Ash Carter, *Department of Defense Cybersecurity Culture and Compliance Initiative*, September 2015, 3, http://www.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf.

[13] Ibid, 8.

[14] Hon. Deborah Lee James and Gen Mark A. Welsh, *USAF Strategic Master Plan*, May 2015, 53, http://www.af.mil/Portals/1/documents/af%20events/2015/Strategic_Master_Plan.pdf.

[15] Lt Col Dave Canady, "Cyber Squadron of the Future," HAF/A6CF briefing slides, May 2014, 2-3, http://www.safcioa6.af.mil/shared/media/document/AFD-140512-040.pdf.

[16] Bender, *Air Force Info Dominance Flight Plan*, 21.

[17] Lt Col Scott Bonzer and Lt Col Daniel Bourque, "Air Force Aggressor Training for Cross-Domain Threats Prepares Airmen for Tomorrow's Victories," Air and Space

Power Journal web article, accessed 11 December 2015,
http://www.airpower.maxwell.af.mil/article.asp?id=165.

Bibliography

Bender, Lt Gen William J. *Air Force Info Dominance Flight Plan: The Way Forward for Cyberspace/IT in the United States Air Force*, 1 May 2015, 21 and 30. http://www.safcioa6.af.mil/shared/media/document/AFD-150610-015.PDF.

Bonzer, Lt Col Scott, and Bourque, Lt Col Daniel. "Air Force Aggressor Training for Cross-Domain Threats Prepares Airmen for Tomorrow's Victories." Air and Space Power Journal web article, accessed 11 December 2015. http://www.airpower.maxwell.af.mil/article.asp?id=165.

Brimley, Shawn. "Promoting Security in Common Domains." *Washington Quarterly* 33, no. 3 (July 2010): 121. doi:10.1080/0163660X.2010.492725.

Bryant, Col William D. "Defending the Walls: Active Cyber Defense of Mission and Weapons Systems." Working paper, 14 Sept 2015, 3.

Canady, Lt Col Dave. "Cyber Squadron of the Future." HAF/A6CF briefing slides, May 2014, 2-3. http://www.safcioa6.af.mil/shared/media/document/AFD-140512-040.pdf.

Charles, Staff Sgt. Michael. "Hacking away at tomorrow's threats: Red Flag incorporates cyber domain." 99th Air Base Wing Public Affairs news release, 6 March 2013. http://www.nellis.af.mil/news/story.asp?id=123338589.

Dempsey, Gen Martin E., and Carter, Hon. Ash. *Department of Defense Cybersecurity Culture and Compliance Initiative*, September 2015, 3. http://www.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf.

Jabbour, Kamal, and Muccio, Sarah. "On Mission Assurance." In *Conflict and Cooperation in Cyberspace*, edited by Panayotis A. Yannakogeorgos and Adam B. Lowther, 109. Boca Raton, FL: Taylor & Francis, 2014.

James, Hon. Deborah Lee, and Welsh, Gen Mark A. *USAF Strategic Master Plan*, May 2015, 53. http://www.af.mil/Portals/1/documents/af%20events/2015/Strategic_Master_Plan.pdf.

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

Poirier, Col William J., and Lotspeich, Maj James. "Air Force Cyber Warfare - Now and the Future." *Air and Space Power Journal* 27, no. 5 (September-October 2013): 87. http://www.airpower.maxwell.af.mil/digital/pdf/issues/2013/ASPJ-Sep-Oct-2013.pdf.

Vautrinot, Suzanne M. "Sharing the Cyber Journey." *Strategic Studies Quarterly* (Fall 2012): 79-80. http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf.